(U) Cryptologic Almanac 50th Anniversary Series

(U) Madame X: Agnes in Twilight,The Last Years of the Career of Agnes Driscoll, 1941-1957.

(U) In cryptology, much like in any profession that emphasizes intellectual agility and extreme concentration, there probably comes a point at which the codebreakers, no matter how good they were, find themselves worn out and overmatched. At that point, the choices are to move to a different job, perhaps to manage, or to teach, or else to continue to attack codes and ciphers, knowing that one's abilities are diminishing.

(U) For almost 20 years, Mrs. Driscoll successfully decrypted Japanese naval and diplomatic codes and cipher systems, including the Orange machine. Then, in a surprise move in October 1940, she was shifted from the JN-25 problem, in which progress was being made, and put in charge of a team working German naval systems, principally the Enigma. From this point she disappears from the limelight. What happened to the Navy's premier cryptanalyst after 1940? Did she simply disappear in the huge complex that wartime navy cryptology became? Or was it that she was overmatched?

(U) In late 1940, the United States was neutral in the conflict raging in Europe, but President Roosevelt considered the Nazis the greatest threat to the country. Britain was beleaguered in the Atlantic and the Mediterranean theaters. Many Americans believed that England could not hold out. Yet, FDR knew England's survival was America's best defense. He approved meetings and exchanges designed to help London. These actions certainly stretched the notion of a "neutral" America. One of the most important was the famous "destroyers-for-bases" deal in which the U.S. Navy transferred 50 overage destroyers to Britain for rights to naval bases in the Western Hemisphere. At another meeting on 31 August 1940, a U.S. Army officer offered to share cryptanalytic information with the British. Within 10 days both sides agreed to set up an exchange.

(U) However, there was a major dissenting voice regarding the proposed exchange - the U.S. Navy's cryptologic organization, OP-20-G. Its chief, Lieutenant Commander Safford, at first had agreed to it. Within months, however, he changed his mind and refused to give anything to the British. Furthermore, he demanded that they give the U.S. Navy complete access to their successes! In November he threatened not to send anyone to the exchange conference scheduled for next spring in Great Britain.

(U) Safford's change of attitude makes it difficult to understand why he formed a German naval section under Driscoll. Was it meant as the receiving end of an envisioned exchange program, or was it an attempt by the Navy to create its own German cryptanalytic effort, free of any reliance on the British? Whatever the reason, Safford and Driscoll believed that little good would come from the British. It also seems that Driscoll had convinced Safford that she could exploit German naval traffic. This may have reinforced his resolve not to participate in the exchange meeting. (The navy eventually sent two junior officers as part of the exchange team.)

(U) Driscoll's optimism in breaking German systems may have resulted from ignorance of the scope of the cryptanalytic problem facing her. The U.S. Navy had little intercept capability for the Atlantic area and lacked German naval traffic to exploit. It was ignorant of German cryptographic systems; it had no copy of a current Enigma machine. Her team had only five members. After Pearl Harbor, it would expand to 15; this was the same size as the team working Italian naval communications, but only a fraction the size of those working Japanese systems. In short, Mrs. Driscoll was starting with few resources and an uncertain purpose.

(U) It appears that she based her cryptanalytic attack on some rather startling assumptions: (1) that the German system was a simple machine (perhaps not unlike the commercial Enigma with which she was familiar); and (2) that the navy could not rely on captured crypto-material, nor expect breakthroughs from operator errors. Instead, she proceeded on the premise that a "catalog" approach would allow for a full-time exploitation of German naval traffic. Although the exact nature of her catalog is unclear, it seems to have involved the taking a known word and produce all possible encryptions of it. An encrypted message then would be searched for a match to the catalog.

(U) In August 1941, Commander Alistair Denniston of the British Government Code & Cipher School visited OP-20-G to urge the Americans to do only cryptanalytic research on German systems. The British had managed finally to exploit the naval Enigma in May, but had not told the Americans. Denniston met with Driscoll, who told him she was not interested in British help. She said her catalog attack would be the way to exploit the Enigma. She told him that when the catalogs were completed, she would need only a few dozen people to solve messages in just days. Considering the British effort involved hundreds of people and a number of "bombes" to beat Enigma, her claim seemed incredible to Denniston. He tried to explain to her that this approach had already been tried and discarded as unlikely to produce enough hits by which daily Enigma settings could be recovered. Driscoll admitted that she did not understand all of the Enigma's operations and needed some help. Denniston promised to send additional information when he returned to England. But it was clear that there was no "meeting of the minds" between the two. Upon his return he would report, with a bit of irony, that she was "the best they [the Americans] had."

(U) For the next several months, the British sent technical information to OP-20-G, including a paper analog of the Enigma. Their queries on the status of Driscoll's effort went unanswered. By late 1941, it appears that optimism over her catalog approach faded. A team of scientists from MIT arrived at OP-20-G to discuss computing machine designs and needs. They were told that her problem was "not important." By spring of 1942, the situation had changed in several ways. For one, the Germans had gone to a four-wheel Enigma, rendering Mrs. Driscoll's research almost moot. In February, Joseph Wenger, who initiated a new cooperative attitude with the British, replaced Safford. He brought in a new set of mathematically oriented cryptanalysts, such as Howard Engstrom and Robert Ely, to head up a new anti-Enigma working group. In April 1942, this group met with the British and, without consulting with Mrs. Driscoll, embarked on their own research. Within 5 months, they arrived at a solution, which was almost exactly the same as the earlier British one. The subsequent American bombe was designed to exploit their breakthrough.

(S//SI) Around April 1943, Mrs. Driscoll was transferred from the Enigma problem to work on the Japanese military attaché machine, known as Coral. This system succumbed to American cryptanalysts two months later, but it is unlikely that she influenced the outcome. After this, she appears to have been moved into a machine support division - GM - within OP-20-G. In April 1944, Mrs. Driscoll was transferred to the project known as the Russian Language Section (OP-20-G-50). This was the U.S. Navy's equivalent of the army's Russian Diplomatic Section that eventually produced the Venona breakthrough. She headed up the small machine support group attached to "50."

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(S//SI) In March 1945, her team "was removed from the rolls" of their old section and rolled into "50." She disappears from the records until June 1946. An entry in the unit history notes that all Russian [redacted] traffic from OP-20-G was to be turned over to Mrs. Driscoll, presumably for her to attempt to exploit. At this time, she headed up the Special Research Team "A" of OP-20-G's Cryptanalytic Research Section, N-3.

(S//SI) [redacted] A report by N-3 noted that the effort involving Mrs. Driscoll was to be "returned" to the army. Sometime in late 1949, Cecil Phillips, who had made the original cryptanalytic breakthrough on Venona, went to see if anything of value could be gotten from her work [redacted]

(C//SI) In 1949 the Armed Forces Security Agency was formed. The army and navy cryptologic organizations transferred a number of their luminaries over to the fledgling AFSA; among them was Agnes Driscoll. She moved through a series of offices, mostly special research areas, winding up in the Technical Consulting Group, ironically led by Frank Raven, who, 9 years earlier as a navy lieutenant, had worked for her on the Enigma

problem.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

~~(C)~~ In 1952, when NSA was formed, she was transferred to the Technical Projects/Services Group, an adjunct research office for Operations. In 1954, she moved to the Pacific Division. There she developed some machine support for analysts working communications targets in [redacted] Asia. In 1956, she was part of some of the first contingents to move to NSA's new location at Fort Meade. However, within a year, at age 68, she retired. Sadly, her retirement was unnoticed by the Agency. She remained in the Washington area. Mrs. Driscoll passed away in September 1971, her death overlooked by NSA. She was buried next to her husband in Arlington Cemetery.

[(U//~~FOUO~~)Robert J. Hanyok, Center for Cryptologic History, 972-2893s, rjhanyo]

Almanac 50th Anniversary Series

Content Owner: Feedback
Web POC: Feedback

Last Modified: by nsr
Last Reviewed: February 28, 2003
Next Review: 365 days